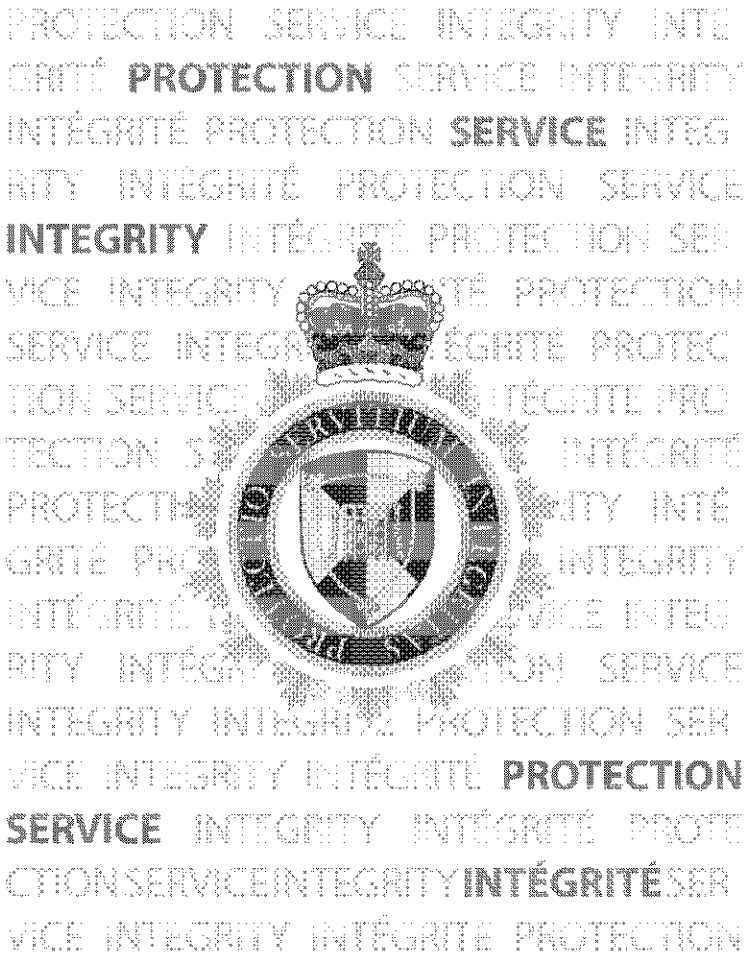
CBSA Lookout Policy

June 2013



PROTECTION • SERVICE • INTEGRITY

Canada

POLICY STATEMENT

1. It is the policy of the Canada Border Services Agency (CBSA) to:

- Issue lookouts in order to provide reliable and timely intelligence on threats and support informed CBSA decision-making on the entry to Canada of persons, goods, conveyances and on exports, as well as to support investigations and enforcement decisions, and additionally, to support Citizenship and Immigration Canada (CIC) decision-making on visa issuance and on status applications;
- Create lookouts that are relevant to the CBSA's jurisdiction;
- Disseminate alerts to field officers to bring to their attention more immediate threats;
- Manage lookout information in accordance with the *Privacy Act,* relevant legislation, and CBSA policies on information sharing; and
- Ensure the integrity of the information contained in the lookouts by putting into place categories that identify where the lookout originates, implementing new requirements for issuing, maintaining, reporting and closing, and implementing new review periods.

AUTHORITY

2. The authority to issue lookouts, cautions and alerts is derived from the CBSA's mandate to provide integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including food, plants and animals, which meet all the requirements under its program legislation.

BACKGROUND

3. At an automated Port of Entry (POE), individuals and conveyances are queried by Border Services Officers (BSOs) stationed at the Primary Inspection Line (PIL) as part of their examination/release procedure. The query, carried out through the Integrated Primary Inspection Line (IPIL) reveals to the primary officer whether a lookout exists.

4. At POEs, BSOs shall refer lookouts for mandatory secondary examination.

5. The secondary officer is responsible for carrying out any specific instructions that the lookout may convey and reporting the interception and its results immediately following the event or as soon as possible thereafter.

PURPOSE AND SCOPE

6. The purpose of this policy is to set out the key requirements, under which CBSA lookouts are issued, maintained and closed.

7. This policy applies to all CBSA employees who issue, assess or use lookouts.

8. CIC recognizes that this policy applies to those CIC Officers who are authorized to issue, assess or use lookouts. Therefore, references to "CBSA" in this policy shall also apply to CIC.

POLICY GUIDELINES

General

9. The CBSA is accountable for the information contained in lookouts. Therefore, resources within the Agency will, to the fullest extent possible, apply a lookout assessment process (see Lookout Standard Operating Procedures (SOPs) Appendix A) to incoming information prior to issuing a new lookout or when reviewing existing lookouts.

10. Lookouts are to be accessed by officers solely to support decision making under the relevant legislation. They are not to be accessed for any purpose falling outside their assigned duties, or with the intention of contravening any policy or instruction. Contraventions will result in the application of appropriate sanctions.

11. When a lookout reaches the end of its lifecycle and is archived, destruction of related sensitive documents must be in accordance with *CBSA's Information Management Policy* effective as of November 28, 2012. This does not preclude the investigating CBSA office from keeping original records relating to the lookout documents.

Lookout Descriptors

12. CBSA lookouts are to be identified by category, CBSA program legislation and type, indicating where a lookout originates, the governing legislation, the type of information, and the intelligence used in the creation of the lookout.

13. All lookouts, regardless of category shall be considered relevant, accurate, valid, and demand serious attention by BSOs.

Lifecycle of a Lookout

14. A CBSA lookout has a "lifecycle" consisting of issuance, maintenance, review, reporting and closing.

15. The procedures for issuance, maintenance reporting and closing will attest to the high standards applied by the CBSA to all lookouts, regardless of category or type.

16. Lookouts shall be reviewed shortly before or on the day the lookout is expected to expire and when the subject of the lookout is intercepted.

17. Lookouts may be extended if still required and/or may be modified if information needs to be added, changed or deleted.

18. When lookouts are no longer required, they should be closed, cancelled, expired, or archived. Access to cancelled, expired or archived lookouts, with the exception of the ACROSS, is restricted to enforcement and intelligence officers.

Lookout Validity and Review Periods

19. It is the policy of the CBSA that lookout information will be reassessed at regular intervals for reliability, accuracy and relevance.

20. The CBSA is appointed to administer and/or enforce various Acts of Parliament. The validity periods will vary from Act to Act. Appendix C of the SOPs outlines the range of lookout validity periods from seven days to ten years, depending on the type of lookout, the system in which it is input and the officer's judgement.

21. Review periods for lookouts are specified in Section 3 and Appendix C of the SOPs.

Attachment of Cautions to Lookouts

22. Lookouts with officer safety cautions must be referred to the regional office where the subject is most likely to be intercepted for validation, issuance and maintenance. However, in exigent circumstances, where interception is imminent and an intelligence officer cannot be reached in a timely manner, BSOs, may attach cautions to lookouts with the approval of their supervisor. CBSA and CIC officers will carefully evaluate the accuracy of information supporting the need for the caution.

Armed and Dangerous Cautions

23. Lookouts with Armed and Dangerous (A&D) Cautions are issued by CBSA Intelligence Officers in consultation with the Border Operations Centre.

24. An "Armed and Dangerous" caution should only be issued where the sum of available information and intelligence provides reasonable grounds to believe that an individual is both armed and likely to use armed force if encountered.

25. In determining whether to issue an "Armed and Dangerous" caution versus another caution such as "Violent" or "Known to Carry a Weapon", both the subject's present situation and past history must be assessed.

26. A lookout containing an armed and dangerous safety caution will refer to one person only.

Issuance of Alerts

27. Alerts may be disseminated to any POE, independent of lookouts, in response to intelligence that indicates the approach of a more immediate threat, where there is insufficient time to prepare a lookout or where intelligence is insufficient to support the preparation of a lookout on a specific individual or shipment.

28. Alerts may be issued to Inland Enforcement Officers and / or CIC where appropriate, pertaining to individuals or threats inside Canada.

29. Alerts may be issued to overseas offices, where appropriate, pertaining to individuals or threats outside Canada.

Dispute Resolution

30. In any case where there is a dispute regarding the issuance or review of a lookout with an officer safety caution, that lookout shall be issued or maintained with the higher level of officer safety caution sought, pending a full review of the case according to the dispute resolution mechanism described in Section 7 of the CBSA Lookout SOPs.

Disclosure of Information

31. Lookout or alert information is not to be shared with any person or organization except as provided for under the *Privacy Act*, Section 107 of the *Customs Act*, D1-16(2), or the information sharing provisions such as the *Statement of Mutual Understanding on Information Sharing* (among CIC, the United States [US] Immigration and Naturalization Service, and the US Department of State) and the *Memorandum of Understanding on API/PNR Sharing*. Officers may also be guided by the provisions of CIC's Information Sharing Manual (IN1 and IN2).

Official Languages

32. All officers issuing or maintaining lookouts shall adhere to the requirements of the *Official Languages Act* in determining the language requirements for lookouts.

Roles and Responsibilities

33. Appendix F of the CBSA Lookout SOPs set out the roles and responsibilities of the CBSA and CIC officers and units involved in the lifecycle of lookouts.

APPENDIX - DEFINITIONS

An "**alert**" describes in general a set of indicators or identifiers that may lead an officer to refer a person, shipment or conveyance for examination. The alert is an additional means of making CBSA officers aware that the individual named in a lookout now poses a more immediate threat or that an expected but unidentified arrival (person of vehicle / goods) poses an immediate or relatively short term threat. An alert indicates imminence, i.e., the threat is expected to occur very soon.

To "**archive**" a lookout in the Integrated Customs Enforcement System (ICES) is to move it from expired status to archived status through a system-generated process that places the lookout within the databank library.

To "**audit**" is to implement a performance measurement regime that will ensure that the lookout system is properly evaluated and that the quality of CBSA lookouts as intelligence products is rigorously maintained.

"Border Services Officers" are officers serving at Canadian ports of entry with customs, Canadian Food Inspection Agency (CFIA) and immigration responsibilities.

To **"close"** a lookout is to "expire" a lookout in ICES and to "delete" a lookout in the Field Operational Support System (FOSS).

To "**cancel**" a lookout in ICES is to remove it from the system and to remove relating records and audit or tracking information for that lookout. It is recommended the "cancel" option only be used in ICES when the lookout is incorrect.

A "**caution**" is a short description, attached to a lookout or alert, that brings to the attention of CBSA officers, wherever located, that the individual named in the lookout or alert possesses certain characteristics of special note, or poses potential danger and/or known threat. The BSO is then able to take appropriate measures, at times preventative, as defined in procedures, operational memoranda, or other instructions.

"CIC Officers" for the purposes of the lookout procedures are officers of Citizenship and Immigration Canada serving in Canada or abroad. To "**delete**" a lookout in FOSS is to remove it from the system of record. The information is maintained in the data warehouse. Note that to "delete" a lookout in FOSS is to "close" it under these procedures.

A lookout is "**expired**" in ICES when it is removed from active use and put it into "expired" status because it is no longer valid. If the lookout no longer needs to be active, expiry can be carried out manually. If the lookout has not been extended before the expiry date then it will automatically expire. Expiring a lookout that is no longer required retains the information in the ICES system. It is recommended that wherever possible the lookouts in ICES should be "expired" rather than cancelled. Note that to "expire" a lookout in ICES is to "close" it under these procedures.
To "**extend**" a lookout is to assign an additional validity period and then keep it in active use because the lookout is still valid.

"**Information**" is defined as raw data, an untested statement or unconfirmed report.

"**Intelligence**" is information collected, evaluated and analysed by way of the intelligence process to produce assessments of events, trends and probability of future activities.

An "**interception**" is an encounter between CBSA officers and the entity (i.e., individual, goods, animal plant, food, resource) or conveyance named within a lookout.

A "**lookout**" is a specific intelligence product developed to identify a person, corporation, conveyance or shipment that, according to various risk indicators or other available intelligence, may pose a threat to the health, safety, security, economy, or environment of Canada and Canadians.

- A lookout takes the form of an electronic file record within the ICES, FOSS, or the Accelerated Commercial Release Operations Support System (ACROSS). The lookout will "flag" or identify particular individuals, including corporations, and specific goods, conveyances or shipments. This "flag", in turn, is intended to prompt a closer examination of circumstances. In order for a primary officer to become aware that a lookout exists, and in so doing become aware that the individual, conveyance or goods of interest have arrived, he or she must make use of a query system the IPIL. Officers within Canada and at ports of entry can query FOSS lookouts or input new FOSS lookouts directly. Officers working overseas as Liaison Officers (LOs) can access existing FOSS lookouts via a linkage with GCMS. Note that while similarities exist, targets are not synonymous with lookouts. The process of targeting is a step removed from the intelligence process. Targeters are provided with indicators that are the products of the intelligence process and then make use of these indicators to create targets.

A "**record of interception**" is a system record in the ICES, FOSS or Global Case Management System (GCMS) reporting on an interception and/or an enforcement action taken by CBSA officers. Information contained in this record may include the reason for referral or examination, or other contact, the results of the search (if applicable), interview notes, tombstone data, the action taken, the results of the encounter and the identity of any travelling companions or associates.

To "**review**" a lookout is to examine the threat assessment process that led to the lookout's issuance, with the aim of judging the validity of the lookout in the light of new information. The review will lead to the lookout being extended, modified, expired or cancelled.